

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN THE MATTER OF THE SEARCH OF:

Apple iPhone 8 IMEI 353220104968455; Google
Pixel 3 cell phone MEID 35827509265273; Dell
Latitude laptop; silver Cruzer Mini 1.0GB thumb
drive; & Samsung tablet IMEI 352250115293313
CURRENTLY LOCATED AT THE FEDERAL
BUREAU OF INVESTIGATION, TOLEDO
RESIDENT AGENCY, 420 MADISON
AVENUE, SUITE 800, TOLEDO, OHIO.

Case No. 3:21MJ5187

AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE

I, Alex O. Hunt, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing examination of the suspect, Jason Paul Bauer's electronic devices, described in Attachment A, which were seized by the Federal Bureau of Investigation (FBI) and are currently in the custody of the FBI, and a search warrant authorizing extraction from those electronic devices of electronically stored information described in Attachment B.

2. Your affiant is a Special Agent of FBI, and as such, is an investigative or law enforcement officer of the United States within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure. Affiant is engaged in the enforcement of criminal laws and is

within a category of officers authorized by the Attorney General to request and execute search warrants pursuant to Title 18 U.S.C. §§ 3052 and 3107; and DOJ regulations set forth at Title 28 C.F.R. §§ 0.85 and 60.2(a). I have been a Special Agent of the FBI since 2015 and am currently assigned to the Northwest Ohio Child Exploitation and Human Trafficking Task Force. I was previously employed as a patrol officer and criminal investigator in Georgia from 2009 to 2015. Since 2009, I have received training and have experience in interviewing and interrogation techniques, arrest procedures, search and seizure, search warrant applications, and various other crimes and investigation techniques.

3. All of the information contained in this affidavit is from my own personal observations or investigation, or from other law enforcement officers whom I believe are reliable. This affidavit contains information solely to establish probable cause for a search warrant and does not list every fact known in this investigation.

4. I am investigating JASON BAUER who has committed violations of 18 U.S.C. § 2422(b) Coercion and Enticement, § 2423(b) Travel with Intent To Engage In Illicit Sexual Conduct, and § 2252(a)(2) Receipt and Distribution of Child Pornography. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that fruits, evidence, and instrumentalities, described in Attachment B, of these crimes are located on the DEVICES described in Attachment A.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

5. The property to be searched is: an Apple iPhone 8 IMEI 353220104968455; a Google Pixel 3 cell phone MEID 35827509265273; a Dell Latitude laptop; a silver Cruzor Mini 1.0GB thumb drive; and a Samsung tablet IMEI 352250115293313 (hereinafter referred to as “the DEVICES”). The DEVICES were in Jason Paul Bauer’s possession at the time of his arrest on

July 15, 2021, and are currently located at the FBI, Toledo Resident Agency, 420 Madison Avenue, Suite 800, Toledo, Ohio, in the Northern District of Ohio, Western Division.

6. The applied-for warrant would authorize the forensic examination of the DEVICES, described in Attachment A, for the purpose of identifying electronically stored data, more particularly described in Attachment B.

BACKGROUND ON COMPUTERS AND ELECTRONIC DEVICES

7. As is the case with most digital technology, communications by way of computers, electronic devices, and cellular telephones can be saved or stored. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP client software, among others).

8. In addition to electronic communications, a computer or cellular telephone user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. A forensic examiner often can recover such evidence, which is typically maintained indefinitely until overwritten by other data.

9. The forensic examiner can also determine the applications and software installed on the device, communications between the user of the phone and others, images and videos saved to the device, and any files uploaded or downloaded from the Internet. This information can exist on the device indefinitely unless intentionally deleted by the user.

CHARACTERISTICS OF INDIVIDUALS WHO SEXUALLY EXPLOIT MINORS

10. Based on my own experience and what I have learned from other investigators, I know that the following traits and characteristics are generally found to exist and be true in cases involving individuals who sexually exploit minors:

a. Individuals who engage or try to engage in sexual exploitation of minors or in sexual activity with children typically have a sexual attraction to minors. They receive sexual gratification and satisfaction from sexual fantasies of minors, sexual activity with minors, and sometimes visual depictions of minors that are sexual in nature, sexually suggestive, and/or sexually explicit.

b. Such individuals may collect sexually suggestive and sexually explicit materials of minors, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. These materials fuel their deviant sexual fantasies involving minors.

c. Such individuals may seek out like-minded individuals, either in person or on the Internet, to communicate, trade sexually suggestive or explicit depictions of minors, and/or arrange to meet with other like-minded individuals for the purpose of sexual activity with minors. This contact not only helps these child exploiters to rationalize and validate their deviant sexual interest and associated behavior, it affords them the ability to find minors with whom they can engage in sexual activity and to make arrangements to engage in sexual activity with that minor. The different Internet-based vehicles used by such individuals to communicate with each other include, but are not limited to, P2P, e-mail, e-mail groups, bulletin boards, IRC, newsgroups, instant

messaging, social media, and other similar vehicles.

d. Individuals who engage or try to engage in sexual exploitation of minors or sexual activity with children may maintain books, magazines, newspapers and other writings, in hard copy or digital medium, on the subject of sexual activities with minors as a way of understanding their own feelings toward minors, justifying those feelings and finding comfort for their illicit behavior and desires. Such individuals rarely destroy these materials in their entirety because of the psychological support they provide.

e. Such individuals may collect, read, copy, or maintain names, addresses (including e-mail addresses), phone numbers, or lists of their victims, or other persons who have advertised or otherwise made known, online or otherwise, that they have similar sexual interests, which may be maintained as a means of personal referral, exchange, or commercial profit. These names may be maintained in notebooks, on computer storage devices, or merely on scraps of paper.

f. Such individuals or individuals who maintain sexually suggestive or explicit materials may go to great lengths to conceal and protect such material from discovery, theft, and damage. This may include storing it in deceptively named apps, files, and/or folders, and/or maintaining it in off-site storage, such as the cloud, which makes the material accessible even as they go from their residence to vehicle to office, and back again.

g. Given the ubiquity of computers and smart devices, as well as their smaller, more compact size (e.g., cell phones, SD cards, or thumb drives), individuals interested in sexually exploiting minors or engaging in sexual activity with a minor typically have

illicit material and evidence of communications with others about such illicit activity on at least one, but typically more than one electronic device. This is especially true as small mobile devices, like a cell phone, can go where the suspect goes, whether it is from his residence to his vehicle to his workplace, and back again. Other electronic devices, such as a home or workplace computer, which may typically remain at one location, can also contain similar illicit communications and/or material about the sexual exploitation of minors.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

11. Searches and seizures of evidence from computers, electronic devices, and cellular telephones commonly require agents to download or copy information from these devices and their components or seize most or all electronic items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

- a. Computer, and cellular telephone, storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and
- b. Searching computer, electronic device, and cellular telephone systems for criminal evidence is a highly technical process requiring expert skill and a properly

controlled environment. The vast array of electronic hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer, electronic device, and/or cellular telephone system is an exacting scientific procedure, which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer, electronic device, and cellular telephone evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

12. To fully retrieve data from a computer, electronic device, and/or cellular telephone system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). The monitor(s) are necessary for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).

13. In addition, there is probable cause to believe that any computer, electronic device, and/or cellular telephone and its storage devices, the monitor, keyboard, printer, modem, router, or any other computer hardware or software found at the PREMISES are all evidence and instrumentalities of the crimes and should all be seized as such.

SEARCH METHODOLOGY TO BE EMPLOYED

14. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is

a non-exclusive list, as other search procedures may be used):

- a. on-site triage of computer systems to determine what, if any, peripheral devices or digital storage units have been connected to such computer systems, as well as a preliminary scan of image files contained on such systems and digital storage devices to help identify any other relevant evidence or potential victims;
- b. examination of all of the data contained in such computer hardware, computer software, or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- c. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- d. surveying various file directories and the individual files they contain;
- e. opening files in order to determine their contents;
- f. scanning storage areas;
- g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and
- h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

15. Based on my knowledge, training and experience, and on the training and experience of other officers upon whom I rely, I know that electronic devices such as cellular telephones can store information for long periods of time. Similarly, web pages that have been viewed via the Internet and other internet usage history are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

16. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage device or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.

- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how an electronic device was used, the purpose of its use, who used it, and when.
- d. Identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of what may be searched and seized under the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

17. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit a complete forensic examination of the devices. The examination may require the use of a variety of techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

18. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion into a premises.

PROBABLE CAUSE

19. Between July 12, 2021 and July 15, 2021, an individual with the KiK username "offroadguy69," using the display name "Jase G," later identified as JASON PAUL BAUER, answered FBI OCE's advertisement by sending a KiK message. OCE and Bauer thereafter

engaged in back-and-forth messaging on KiK, during which Bauer sent an image of child pornography. A summary of the conversation below is used simply as a reference; the recorded chats should be the final authority. Relevant portions of the conversation between OCE and Bauer (“Subject”) are as follows:

....

OCE: What are you into

Subject: Young amateurs, breeding, sneak pics, stories, dick pics,

....

OCE: I’m into actual play It’s not for everyone

Subject: As in you’d share her?

OCE: Ya of I can trust you. I’ve shared before

Subject: Oh I’d love that!

....

OCE: What do you want to do with her

Subject: First just get her nude. Haven’t seen a nude dau before.

Subject: Then give her a bath or have her shower me.

Subject: Touching and feeling her.

Subject: And have her wash me.

OCE: Hell ya man, that’s hot

Subject: Then towel her off and get in bed.

Subject: I want to taste her

OCE: Mmm you can

Subject: Explore her up close. See her cute kitty.

....

Subject: Any fur on her or bald?

OCE: Lol dude she's 7

....

Subject: Do you cum inside?

Subject: Can i?

....

Subject: Awesome! Or all 3 of us could shower and play together.

Subject: Will she suck me?

....

Subject: Id love to join you.

OCE: Where do u live

Subject: Indiana

Subject: You?

OCE: How old are you?

OCE: Ohio

Subject: 40

OCE: We can be free this afternoon if you are

Subject: What part of Ohio?

OCE: Toledo

Subject: Damn. That's about 5 hrs. Would need a little planning to get there

OCE: Oh damn..

Subject: But could be worth it to me.

....

Subject: How would the meet up go?

OCE: We can grab a hotel, meet up on the lobby or parking lot, then go up to the room where Hannah will be

OCE: Do you have pics or vids?

Subject: Yeah what sort of pics are you looking for.

OCE: Younger the better

Subject: *[sent photograph of child sexual abuse material, depicting a naked prepubescent female, standing, with her vaginal region exposed]*

OCE: Nice

OCE: Where do you get ur stuff

Subject: You have anything to share?

OCE: Not on this phone

....

OCE: What do you have

Subject: Randoms I found over the years

OCE: Cool

OCE: Laptop?

Subject: USB

OCE: Cool, you can plug into my lt

....

OCE: Goe [sic] do u hide it from her

OCE: How

Subject: USB [with winking face emoji]

....

7. On July 15, 2021, OCE and Bauer arranged to meet the OCE and OCE's purported seven-year-old daughter at the Motel 6 in Toledo, Ohio, in the Northern District of Ohio,

Western Division, for the purpose of engaging in sexual conduct with the minor. At approximately 1:25 p.m., Bauer arrived at the prearranged location, the Motel 6, in a Hertz rental car, a silver Chevrolet Trailblazer with Illinois license plate FP134640. Surveillance teams observed Bauer as the driver in the vehicle based on the picture that Bauer had previously sent to the OCE. Bauer messaged the OCE and informed the OCE that he had arrived and was in a silver Trailblazer. Bauer was then arrested by FBI Agents and Task Force Officers. Inside of his vehicle were the DEVICES, as described in Attachment A. Bauer also had a bag of Skittles in his pocket, which was consistent with what he told the OCE in messages he would bring for the minor.

8. Following his arrest, Bauer was interviewed at the Toledo FBI office. After Bauer was advised of his Miranda rights, waived them, and agreed to speak with investigators, he admitted that he drove from Indiana to the Motel 6 in Toledo, Ohio to meet with whom he believed to be a father with a seven-year-old-daughter to have sex with the minor. Bauer also admitted to bringing a thumb drive that contained child sexual abuse material or child pornography. Bauer admitted to sending an image of child pornography to the father of the seven-year-old daughter during their chats before arriving that day. He said that the image was on the thumb drive that he had with him when he came to Toledo that day. When presented with a copy of the chats between him and the OCE, Bauer identified his Kik account as being the one corresponding with the OCE and also identified the child pornography image as the one he had sent in their chats. Bauer admitted to renting a car today to make the drive to Toledo. He stated that he lied to his “significant other” when he said that the trip to Toledo was “a work trip.” Bauer admitted to having condoms in his bag in his vehicle, although claiming that they were there even before arranging to come to Toledo.

CONCLUSION

27. Based on all of the above, Affiant respectfully submits that there is probable cause to believe that evidence, fruits, and contraband, described in Attachment B, of the criminal offenses—namely, violations of 18 U.S.C. § 2422(b), Coercion and Enticement, 2423(b) Travel With Intent To Engage In Illicit Sexual Conduct, and 2252(a)(2) Receipt and Distribution of Child Pornography—are located on the DEVICES described in Attachment A.

28. Based on the foregoing, Affiant requests issuance of a search warrant for the DEVICES described in Attachment A to search for the evidence described in Attachment B.

Respectfully submitted,



SA Alex O. Hunt (FBI)

Sworn to via telephone after submission by
reliable electronic means pursuant to Fed.Cr.R.
4.1(d)(3) and 41 on July ~~20~~, 2021.



Honorable Darrell A. Clay
UNITED STATES MAGISTRATE JUDGE